Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

54. (Previously Presented) A computer-implemented method for managing access to electronic documents, comprising:

associating a first key with an encrypted document decryption key, the encrypted document decryption key being associated with an encrypted document, the encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the encrypted document, the first key being usable to decrypt the encrypted document decryption key;

encrypting the first key to produce an encrypted first key;

providing the encrypted first key in a first access controlled manner to users for use in opening the encrypted document;

associating with the encrypted first key a second key that can be used to decrypt the encrypted first key; and

providing the second key in a second access controlled manner to users for use in opening all documents that can be opened through use of the first key, the second access controlled manner being distinct from the first access controlled manner,

wherein providing the second key in an access controlled manner comprises sending information used to synthesize the second key in rights management information, and wherein the rights management information provides a license and defines a set of permission rights associated with the license, and wherein the set of permission rights specifies a right allowing another key to be associated with the rights management information so that a holder of such a key has access to the first key.

55. (Previously Presented) The method of claim 54, wherein the set of permission rights specifies a right allowing a holder of the first key to add to a second encrypted document a

second encrypted document decryption key that can be decrypted by the first key and, when decrypted by the first key, yielding a second document decryption key that is usable to decrypt the encrypted second document.

56. (Previously Presented) The method of claim 54, wherein multiple keys are usable to decrypt the encrypted document decryption key directly or indirectly, wherein the multiple keys are provided to users in rights management information, and wherein the encrypted document specifies permission rights including a right to override one or more permission rights specified by rights management information for any one or more of the multiple keys.

57. (Previously Presented) The method of claim 56, wherein the rights management information comprises a rights management file.

58. (Previously Presented) The method of claim 56, wherein the rights management file is specific to a particular user.

59. (Previously Presented) The method of claim 56, wherein the rights management file is specific to a particular user-operated system.

60. (Previously Presented) The method of claim 54, wherein multiple keys are usable to decrypt the encrypted document decryption key directly or indirectly, wherein the multiple keys are provided to users in rights management information, and wherein the encrypted document specifies permission rights including a right to override one or more permission rights specified by rights management information for any one or more of the multiple keys.

61. (Previously Presented) A computer-implemented method for accessing an electronic document, comprising:

obtaining an encrypted electronic document;

obtaining a collection of three or more keys, the keys including keys that are encrypted, the keys and the document having at least two associations defined between certain pairs of them, where at least one association is a pair consisting of a first key and an encrypted second

key indicates that the first key can be used to decrypt and thereby make usable the second key, where at least one association is a pair consisting of the encrypted second key and an encrypted third key, the association indicating that the decrypted second key can be used to decrypt and thereby make usable the third key, where each association of a pair consisting of an encrypted document decryption key and the encrypted document indicates that the encrypted document decryption key, when decrypted, can be used to decrypt the encrypted document, and where a user has access to and can use certain ones of the keys in the collection;

using the associations to identify at least one key in the collection that is usable, directly or indirectly, to open the encrypted document, and to which the user has access, wherein the associations are represented as a directed graph, with each node representing a key or the document, with one or more nodes representing keys accessible to the user, and with one or more edges pointing to the document, and wherein using the associations to identify at least one key comprises finding a path in the directed graph to the node representing the document from one of the nodes representing keys accessible to the user.

62. (Previously Presented) The method of claim 61, further comprising:

following the path and decrypting each of the keys represented by nodes along the path in turn until an encrypted document decryption key for the document is decrypted.

63. (Previously Presented) The method of claim 62, wherein each encrypted key is identified by two IDs, including a first ID corresponding to the encrypted key and a second ID corresponding to another of the keys capable of decrypting the encrypted key.

64. (Previously Presented) The method of claim 63, wherein two or more second IDs correspond to the same first ID, and each of the two or more second IDs and the encrypted keys to which they correspond are stored as separate entries in an array of entries, each of the entries being indexed by the same first ID.

65. (Previously Presented) The method of claim 63, wherein each encrypted key is stored with the corresponding second ID as an entry in an array and each entry is indexed by the corresponding first ID.

66. (New) A system for managing access to electronic documents comprising:

one or more processors, and

a computer-readable medium comprising instructions to cause the processors to perform operations comprising:

associating a first key with an encrypted document decryption key, the encrypted document decryption key being associated with an encrypted document, the encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the encrypted document, the first key being usable to decrypt the encrypted document decryption key;

encrypting the first key to produce an encrypted first key;

providing the encrypted first key in a first access controlled manner to users for use in opening the encrypted document;

associating with the encrypted first key a second key that can be used to decrypt the encrypted first key; and

providing the second key in a second access controlled manner to users for use in opening all documents that can be opened through use of the first key, the second access controlled manner being distinct from the first access controlled manner,

wherein providing the second key in an access controlled manner comprises sending information used to synthesize the second key in rights management information, and wherein the rights management information provides a license and defines a set of permission rights

associated with the license, and wherein the set of permission rights specifies a right allowing another key to be associated with the rights management information so that a holder of such a key has access to the first key.

67. (New) The system of claim 66, wherein the set of permission rights specifies a right allowing a holder of the first key to add to a second encrypted document a second encrypted document decryption key that can be decrypted by the first key and, when decrypted by the first key, yielding a second document decryption key that is usable to decrypt the encrypted second document.

68. (New) The system of claim 66, wherein multiple keys are usable to decrypt the encrypted document decryption key directly or indirectly, wherein the multiple keys are provided to users in rights management information, and wherein the encrypted document specifies permission rights including a right to override one or more permission rights specified by rights management information for any one or more of the multiple keys.

69. (New) The system of claim 68, wherein the rights management information comprises a rights management file.

70. (New) The system of claim 68, wherein the rights management file is specific to a particular user.

71. (New) The system of claim 68, wherein the rights management file is specific to a particular user-operated system.

72. (New) The system of claim 66, wherein multiple keys are usable to decrypt the encrypted document decryption key directly or indirectly, wherein the multiple keys are provided to users in rights management information, and wherein the encrypted document specifies permission rights including a right to override one or more permission rights specified by rights management information for any one or more of the multiple keys.

73. (New) A system for accessing an electronic document comprising:

one or more processors, and

a computer-readable medium comprising instructions to cause the processors to perform operations comprising:

obtaining an encrypted electronic document;

obtaining a collection of three or more keys, the keys including keys that are encrypted, the keys and the document having at least two associations defined between certain pairs of them, where at least one association is a pair consisting of a first key and an encrypted second key indicates that the first key can be used to decrypt and thereby make usable the second key, where at least one association is a pair consisting of the encrypted second key and an encrypted third key, the association indicating that the decrypted second key can be used to decrypt and thereby make usable the third key, where each association of a pair consisting of an encrypted document decryption key and the encrypted document indicates that the encrypted document decryption key, when decrypted, can be used to decrypt the encrypted document, and where a user has access to and can use certain ones of the keys in the collection;

using the associations to identify at least one key in the collection that is usable, directly or indirectly, to open the encrypted document, and to which the user has access, wherein the associations are represented as a directed graph, with each node representing a key or the document, with one or more nodes representing keys accessible to the user, and with one or more edges pointing to the document, and wherein using the associations to identify at least one key comprises finding a path in the directed graph to the node representing the document from one of the nodes representing keys accessible to the user.

74. (New) The system of claim 73, further comprising:

following the path and decrypting each of the keys represented by nodes along the path in turn until an encrypted document decryption key for the document is decrypted.

75. (New) The system of claim 74, wherein each encrypted key is identified by two IDs, including a first ID corresponding to the encrypted key and a second ID corresponding to another of the keys capable of decrypting the encrypted key.

76. (New) The system of claim 75, wherein two or more second IDs correspond to the same first ID, and each of the two or more second IDs and the encrypted keys to which they correspond are stored as separate entries in an array of entries, each of the entries being indexed by the same first ID.

77. (New) The system of claim 75, wherein each encrypted key is stored with the corresponding second ID as an entry in an array and each entry is indexed by the corresponding first ID.

78. (New) A computer program product, tangibly stored on a computer-readable medium, operable to cause data processing apparatus to perform operations for managing access to electronic documents comprising:

associating a first key with an encrypted document decryption key, the encrypted document decryption key being associated with an encrypted document, the encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the encrypted document, the first key being usable to decrypt the encrypted document decryption key;

encrypting the first key to produce an encrypted first key;

providing the encrypted first key in a first access controlled manner to users for use in opening the encrypted document;

associating with the encrypted first key a second key that can be used to decrypt the encrypted first key; and

providing the second key in a second access controlled manner to users for use in opening all documents that can be opened through use of the first key, the second access controlled manner being distinct from the first access controlled manner,

wherein providing the second key in an access controlled manner comprises sending information used to synthesize the second key in rights management information, and wherein the rights management information provides a license and defines a set of permission rights associated with the license, and wherein the set of permission rights specifies a right allowing another key to be associated with the rights management information so that a holder of such a key has access to the first key.

79. (New) The computer program product of claim 78, wherein the set of permission rights includes instructions operable to cause a processor to specify a right allowing a holder of the first key to add to a second encrypted document a second encrypted document decryption key that can be decrypted by the first key and, when decrypted by the first key, yielding a second document decryption key that is usable to decrypt the encrypted second document.

80. (New) The computer program product of claim 78, wherein multiple keys are usable to decrypt the encrypted document decryption key directly or indirectly, wherein the multiple keys are provided to users in rights management information, and wherein the encrypted document specifies permission rights including a right to override one or more permission rights specified by rights management information for any one or more of the multiple keys.

81. (New) The computer program product of claim 80, wherein the rights management information comprises a rights management file.

82. (New) The computer program product of claim 80, wherein the rights management file is specific to a particular user.

83. (New) The computer program product of claim 80, wherein the rights management file is specific to a particular user-operated system.

84. (New) The computer program product of claim 78, wherein multiple keys are usable to decrypt the encrypted document decryption key directly or indirectly, wherein the multiple keys are provided to users in rights management information, and wherein the encrypted document specifies permission rights including a right to override one or more permission rights specified by rights management information for any one or more of the multiple keys.

85. (New) A computer program product, tangibly stored on a computer-readable medium, operable to cause data processing apparatus to perform operations for accessing an electronic document comprising:

obtaining an encrypted electronic document;

obtaining a collection of three or more keys, the keys including keys that are encrypted, the keys and the document having at least two associations defined between certain pairs of them, where at least one association is a pair consisting of a first key and an encrypted second key indicates that the first key can be used to decrypt and thereby make usable the second key, where at least one association is a pair consisting of the encrypted second key and an encrypted third key, the association indicating that the decrypted second key can be used to decrypt and thereby make usable the third key, where each association of a pair consisting of an encrypted document decryption key and the encrypted document indicates that the encrypted document decryption key, when decrypted, can be used to decrypt the encrypted document, and where a user has access to and can use certain ones of the keys in the collection;

using the associations to identify at least one key in the collection that is usable, directly or indirectly, to open the encrypted document, and to which the user has access, wherein the associations are represented as a directed graph, with each node representing a key or the document, with one or more nodes representing keys accessible to the user, and with one or more

edges pointing to the document, and wherein using the associations to identify at least one key comprises finding a path in the directed graph to the node representing the document from one of the nodes representing keys accessible to the user.

86. (New) The computer program product of claim 85, further comprising instructions operable to cause a programmable processor to:

follow the path and decrypt each of the keys represented by nodes along the path in turn until an encrypted document decryption key for the document is decrypted.

87. (New) The computer program product of claim 86, wherein each encrypted key is identified by two IDs, including a first ID corresponding to the encrypted key and a second ID corresponding to another of the keys capable of decrypting the encrypted key.

88. (New) The computer program product of claim 87, wherein two or more second IDs correspond to the same first ID, and each of the two or more second IDs and the encrypted keys to which they correspond are stored as separate entries in an array of entries, each of the entries being indexed by the same first ID.

89. (New) The computer program product of claim 87, wherein each encrypted key is stored with the corresponding second ID as an entry in an array and each entry is indexed by the corresponding first ID.